International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 2

Practical data hiding technique in Covert timing channels

M. Gokul Narayanan, PS. Lokesh, N. Kanimozhi
Department of Computer Science and Engineering,
G.K.M. College of Engineering and Technology, Chennai, Tamil Nadu, India

ABSTRACT

Out of order arrival of packets is an inevitable phenomenon on the Internet. Application performance can degrade to a great extent due to out-of-order arrival of packets Packet reordering is a common phenomenon on the Internet. Moreover, it is handled transparently from the user and application-level processes. In this paper, we propose a novel covert channel technique using the packet reordering phenomenon as a host for carrying secret communications. This makes it an attractive medium to exploit for sending hidden signals to receivers by dynamically manipulating packet order in a network flow. In our approach, specific permutations of successive packets are selected to enhance the reliability of the channel, while the frequency distribution of their usage is tuned to increase stealthiness by imitating real Internet traffic. It is very expensive for the adversary to discover the covert channel due to the tremendous overhead to buffer and sort the packets among huge amount of background traffic. A simple tool is implemented to demonstrate this new channel. We studied extensively the robustness and capabilities of our proposed channel using both simulation and experimentation over large varieties of traffic characteristics. The reliability and capacity of this technique have shown promising results. We also investigated a practical mechanism for distorting and potentially preventing similar novel channels.

Keywords: *Packet Sequence, data hiding transference, Covert timing channel, Secrete communications*

I. INTRODUCTION

In the past few years, the Internet has exploded to include millions of users communicating with thousands of applications using hundreds of protocols. However, data transmission has been always characterized by being visible, in the open and available to anyone to collect and analyse. All data protection techniques focus on protecting the payload rather than hiding the existence of the channel itself. The adversary can easily find the channel and recover the information. The adversary just randomly places an observation points or monitor at random times and easily detect presence of channel in the network. All packets are transmitted over the internet in sequence order. We propose a technique that can use the unconventional channel of packet order to be our covert communication medium. User data split into small amount of information's. This small amount of information is called packet. The Source provides unique number for each packet. These packets are encoded using base64 algorithm. Source creates a block used to transmit a packet. The packets are shuffle and then placed in the blocks so that every block will contain shuffled packets. Source finds all possible paths to reach the destination. Source sends a block to Destination. Source does not send all blocks to the same path. Each block sends in different path. Source generates a codeword for all bocks. Original order of packet's unique number is called codeword. codeword sends in another channel and the channel send only code word not a block. All blocks contain out-of-order packets. The destination arranges the packet using these codeword. The destination receives all blocks from the source and these blocks are travel

in different channel. Some channel contains more noises so packets are easily loss. Some channel contains very less noise so no loss of packets. Block travel in noise channel the loss some packets that block reach a destination. The destination will find an error. The destination indicates to the source. The source resends a message in low noise path.

II. Related works

A Marcus Völp, Claude-Joachim Hamann and Hermann Härtig (2008) are designed a practically feasible modification to fixed-priority schedulers allows to avoid timing channels despite threads having access to precise clocks. Tarun Banka ,Abhijit A. Bare and Anura P.Jayasumana Out of order arrival of packets is an inevitable phenomenon on the Internet. Sharad Jaiswal, Gianluca Iannaccone, Christophe Diot, Jim Kurose and Don Towsley (2003)are described Measurement and Classification of Out-of-Sequence Packets in a Tier-1 IP Backbone. Myong H. Kang, Ira S. Moskowitz and Daniel C. Lee used MULTI-LEVEL SECURE (MLS)system stores and processes information of different sensitivity levels in a secure manner. Xenofon Fafoutis, Evgeny Tsimbalo and Robert Piechocki (2014) the project was used to Timing Channels in Bluetooth Low Energy. Nischal M. Piratla and Anura P. Jayasumana project concept is Reordering of packets due to multipath forwarding an analysis. Steven J. Murdoch and Stephen Lewis (2005) are explained the method Embedding Covert Channels into TCP/IP. Ang Chen,W. Brad Moore and Hanjun Xiao (2013) implemented the concept of Detecting Covert Timing Channels with Time-Deterministic Replay. L. Gallucio,

G. Morabito, and S. Palazzo, “Exploiting timing channels in intra-body sensor networks,”, in Proc. IEEE Global Commun.(2012)

III. Proposed system

The project proposes a technique that can use the unconventional the covert channel from the huge amount of background traffic. If the adversary just randomly channel of packet order to be our covert communication medium. By manipulating the order of packets sent over the network at the sender-side, we emulate the packet reorder phenomenon which takes place naturally. And project is used to the secure communications of data by encoding the packets using the Base64 algorithm.

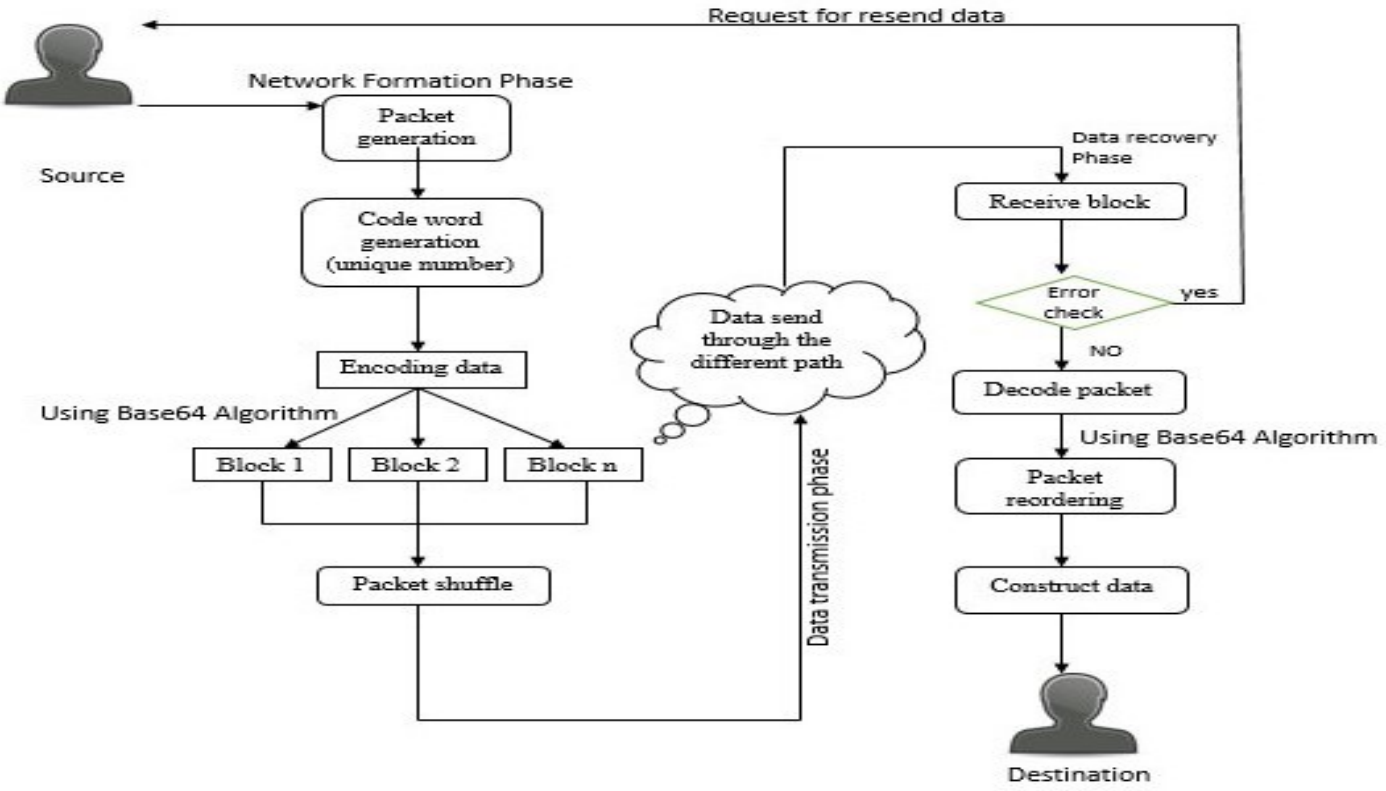

Fig. 1 Architecture diagram

A. *Network formation and Packet Generation Phase*

In this module, create a network formation. We consist multi-hop network contains number of nodes. Each node has some range. The node can communicate its range. Any one node range intersect with another node range it define both are neighbour. One node can have more number of neighbours. The destination is not a neighbour of source can't send information directly to the destination. It sends an information to its neighbour and the neighbour send an information to another neighbour and then finally it reaches to destination. Source find a path to reach destination.

B. *Encoding and shuffling packets*

In this module, user information is not directly send to the destination. User data split into small amount of information's. These small amount of information is called packet. If the original information is needed, will arrange the packets. But data split into n number of packet. It is difficult to arrange the original order. So the source provides a unique number for each packet. The source transmits a packet in the overt channel the adversary can easily detect the overt channel and recover the data from the channel. The source executes some techniques to avoid these problem. The data convert into packets and the source provide a unique number of each packets then each packet encodes using base64 algorithm. Source creates a blocks. The block contains particular amount of packets. The packets are arranged in block out of order manner.

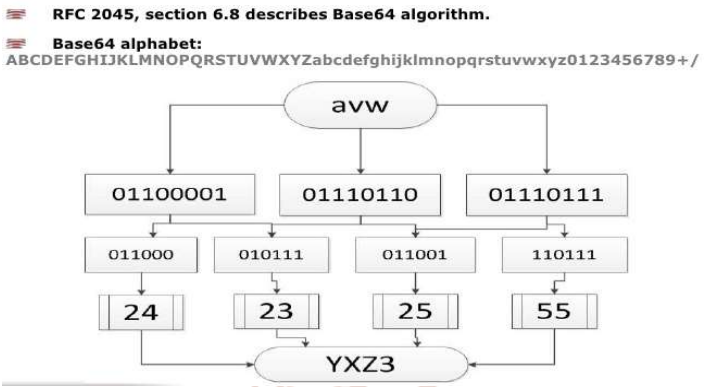

Fig. 2 Working of Base64 Algorithm

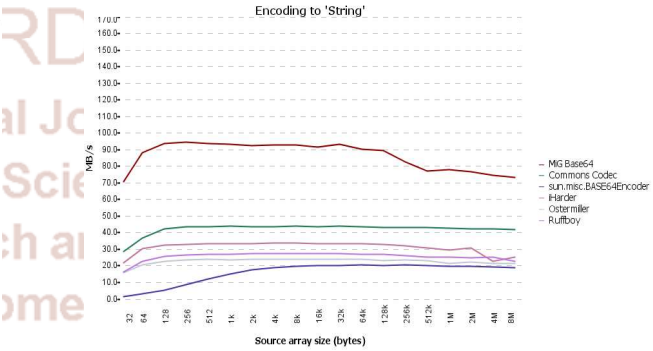

Fig. 3

C. *Data transmission phase*

Source finds all possible paths to reach the destination. Source sends a block to Destination. Source does not send all blocks to the same path. Each block sends in different path. Source generates a codeword for all bocks. Original order of packet's unique number is called codeword. codeword sends in another channel and the channel send only code word not a block. All blocks contain out-of-order packets. Destination receives a blocks from all possible channel and also receive a codeword. The destination decodes an all packets using base64 algorithm and arrange the packet using these codeword.

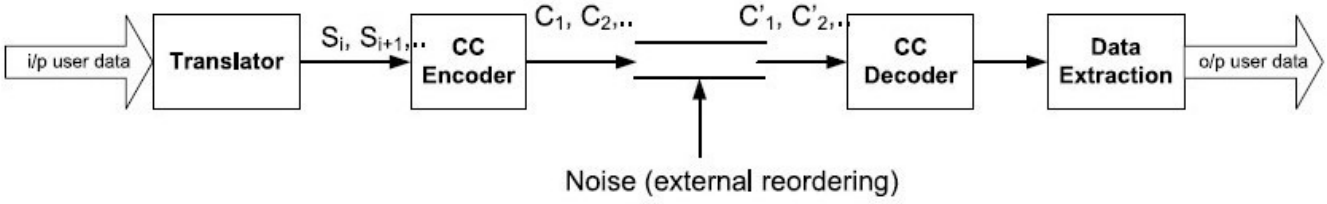

Fig. 4 Data transmission

D. Data Recovery Phase

The destination receives all blocks from the source and these blocks are travel in different channel. Some channel contains more noises so packets are easily loss. Some channel contains very less noise so no loss of packets. Block travel in noise channel the loss some packets that block reach a destination. The destination will find an error. The destination indicates to the source. The source resends a message in low noise path. The destination decodes all packets using base64 algorithm and arrange the original order of these packets using codeword.

TABLE 1: Effect of prevention power on error rate of Covert channel

$d \downarrow \setminus k \rightarrow$	2	3	4	5
1		0.005%	0.02%	0.041
2		0.472%	1.006%	1.475
3	N/A	0.6525%	1.323%	1.966
4		0.75%	1.526%	2.170
5		0.7625%	1.586%	2.425

Conclusions

In this paper, we pursue the possibility of building covert channels that use the packet order as the medium for transmitting hidden signals. Packet reordering is a normal behaviour in the Internet and it is too hard to closely monitor and unlikely to raise suspicions. Moreover, efforts to eliminate it will not be easily implemented due to high cost and lack of incentive. Also, the main causes behind this phenomenon are not likely to vanish nor decrease in the near future. Our proposed channel is designed based on the idea of assigning different symbols to the different permutations a number of consecutive packets can have. By using only, a subset of the permutations, we were able to add error detection and correction capabilities. Subsets used are rotated to evade detection. Any adversary needs a huge cost to detect the covert channel due to the tremendous overhead to buffer and sort the packets among huge amount of background traffic. The code words themselves are selected based on the traffic characteristics to follow closely the innate reordering characteristics of the host channel.

.

REFERENCES

1) El-Atawy, A., Duan, Q. and Al-Shaer, E., 2017. A novel class of robust covert channels using out-of-order packets. *IEEE Transactions on Dependable and Secure Computing*, *14*(2), pp.116-129..
2) M. Allman and E. Blanton. "On Making TCP More Robust to Packet Reordering", ACM Computer Communication Review, 32(1), January 2002.
3) Piratla, N. M., Jayasumana, A. P., and Banka, T., "On Reorder Density and its Application to Characterization of Packet Reordering," Proc. 30th IEEE Local Computer Networks Conference (LCN 2005), Sydney, Australia, Nov. 2005.
4) Y. Liu, D. Ghosal, F. Armknecht, A. Sadeghi, S. Schulz, and S. Katzenbeisser, "Robust and undetectable steganographic timing channels for i.i.d. traffic," in Proc. 12th Int. Conf. Inf. Hiding, Berlin, Germany, 2010, pp. 193–207.
5) S. Jaiswal, G. Iannaccone, C. Diot, J. Kurose, and D. Towsley. Measurement and classification of out-of-sequence packets in a tier-1 ip backbone. Technical Report 02-17, Computer Science Dept., UMass Amherst, May 2002.
6) W. Hu, "Reducing timing channels with fuzzy time," in Proc. IEEE Comput. Soc. Symp. Res. Security Priv., 1991, pp. 8–20.
7) A. Houmansadr and N. Borisov, "Coco: Coding-based covert timing channels for network flows," in Proc. 13th Int. Conf. Inf. Hiding, 2011, pp. 314–328.
8) R. Piechocki and D. Sejdinovic, "Combinatorial channel signature modulation for wireless ad-hoc networks," in Proc. IEEE Int. Conf. Commun. (ICC), June 2012, pp. 4684–4689.
9) S. Cabuk, C. E. Brodley, and C. Shields, "Ip covert channel detection," ACM Trans. Inf. Syst. Security, vol. 12, no. 4, pp. 22:1– 22:29, Apr. 2009.
10) S. Voloshynovskiy and F. Deguillaume, "Information-theoretic data-hiding: Recent achievements and open problems," Int. J. Image Graph., vol. 5, no. 1, pp. 1–31, 2005.
11) S. H. Sellke, C. Wang, S. Bagchi, and N. B. Shroff, "TCP/IP timing Channels: Theory to Implementation," in Proc. IEEE INFOCOM, 2009, pp. 2204–2212.